ComplyPS
Comply Product Security

REGULATION (EU) 2024/2847 · EFFECTIVE 11 DEC 2027

ComplyCRA

Your all-in-one EU Cyber Resilience Act compliance solution

Classify your product, self-assess against Annex I, scan your SBOM for vulnerabilities, run an AI gap assessment, and stay audit-ready — all processed privately on your own infrastructure.

BUILT ON THE OFFICIAL CRA TEXT | OFFLINE & PRIVATE | READY BEFORE DEC 2027 | CLASSIFY IN MINUTES

One platform for the whole CRA journey

The Cyber Resilience Act makes cybersecurity a legal condition for placing connected products on the EU market. ComplyCRA turns that regulation into a guided, step-by-step workflow — from working out whether you are in scope, to closing the gaps, to generating the evidence an auditor expects.

3	22+	24/72h
risk classes handled	requirements checked	reporting templates

What ComplyCRA does

Scope & risk classifier

Answer a few questions to learn instantly whether your product is in scope, which exclusions apply, and its risk class — Default, Important (Annex III) or Critical (Annex IV).

Annex I self-assessment

Work through the essential cybersecurity requirements as a structured checklist, record your justification for each, and get a clear readiness score per product.

AI gap assessment

Upload your policies, technical docs and evidence. A local AI checks them against the CRA and reports coverage, gaps and concrete recommendations — document text never leaves your machine.

Offline SBOM vulnerability scanning

Upload or generate a software bill of materials and scan it against known CVEs and exploited-vulnerability status using a local, offline database — no data sent to third parties.

Live compliance dashboard

See overall coverage across every product, open reporting deadlines, support-period status and what to fix next — all in one readiness view for leadership.

Coordinated Vulnerability Disclosure

Generate a CVD policy and publish a security contact once for your whole company; it counts toward every product's coverage.

Approval-gated reporting

Prepare 24-hour, 72-hour and final reports for actively exploited vulnerabilities and severe incidents, aligned to the ENISA Single Reporting Platform, gated behind multi-person approval.

Technical documentation & DoC

Assemble the technical documentation and EU Declaration of Conformity as you go, and pick the right conformity route for your risk class.

What ComplyCRA does (continued)

Accounts, roles & demo access

Admin-created accounts with clear roles — administrators, full users, and a read-only demo account with a sample project for showing stakeholders.

Private & offline by design

The public site only displays data; all logic, storage and AI run on your own infrastructure. Nothing is self-hostable by others and your evidence stays under your control.

Key CRA dates — and why to start now

Dec 2024

Entry into force

The regulation is law; the framework is fixed and you can plan against final text.

11 Sep 2026

Reporting obligations begin

Duties to report actively exploited vulnerabilities and severe incidents apply first.

11 Dec 2027

Full application

Essential requirements, conformity assessment, CE marking and the Declaration of Conformity apply.

Get CRA-ready with ComplyCRA

Try the scope classifier free — no account needed — or book a live demo to see the full platform, including the AI gap assessment.

Book a live demo

complyps.com/complyps-cra

This brochure is general information about the EU Cyber Resilience Act and the ComplyCRA product; it is not legal advice. Always refer to the official text of Regulation (EU) 2024/2847.